In response to applicant's phone call regarding the last Office action, the following corrective action is taken.

The period for reply of 3 MONTHS set in said Office Action is restarted to begin with the mailing date of this letter.

DETAILED ACTION

This action is in response to the papers filed 3/6/2009.

Response to Arguments

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim 1, 3, 4, 9, 10, 21, 23-25, 26, 28, 31, 33-35, 36, 38 39, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Forslow (U.S. 6,973,057).

With respect to claim 1 Dellmo teaches a cryptographic device comprising: a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) and a communications module (paragraph 0038 i.e. wireless transceiver 50) coupled thereto (see figure 7); said cryptographic module comprising a user network interface (see figure

7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to said user network interface (see figure 2), and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7); said communications module comprising a network communications interface (see paragraph 0035 and 0041-0046) coupled to said cryptographic processor (see figure 7);

Dellmo does not teach said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon.

Forslow teaches said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the

encapsulated communications module command packets to said communications module without performing cryptographic processing thereon (see Forslow figure 2 and column 9 lines 10-28). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have enclosed a command packet within an IP packet to have an efficient way to pass a command packet. Therefore one would be motivated to have enclosed a command packet within an IP packet.

With respect to claim 3, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036).

With respect to claim 4, wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Mitsuoka figure 6A, 6B and column 14 lines 49-67).

With respect to claim 9, wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 10, wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface (see Dellmo figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), and wherein said network communications interface comprises a network LAN interface (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 21 Dellmo teaches communications method comprising: coupling a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) to a network device (see figure 2), the cryptographic module comprising a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to the user network interface (see figure 2), and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to the host network processor (see figure 7); providing a communications module (paragraph 0038 i.e. wireless transceiver 50) comprising a network communications interface (see paragraph 0035 and 0041-0046) coupled to the cryptographic processor (see figure 7);

Dellmo does not teach said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon.

Forslow teaches said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion

for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon (see Forslow figure 2 and column 9 lines 10-28). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have enclosed a command packet within an IP packet to have an efficient way to pass a command packet. Therefore one would be motivated to have enclosed a command packet within an IP packet.

With respect to claim 23, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036).

With respect to 24, wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Mitsuoka figure 6A, 6B and column 14 lines 49-67).

With respect to claim 25, wherein the user network interface comprises an Ethernet Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), and wherein the network communications interface comprises a network LAN interface (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 26, Dellmo teaches a communications system comprising: a plurality of network devices coupled together to define a network (see figure 4 and paragraph 0035), and a cryptographic device (see figure 2 element 20) coupled to at least one of said network devices (see figure 2); said cryptographic device comprising a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) coupled to said at least one network device (see figure 2), and a communications module (paragraph 0038 i.e. wireless transceiver 50) coupled to said cryptographic module (see figure 7); said cryptographic module comprising a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to said user network interface (see figure 2), and a cryptographic processor see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7); said communications module comprising a network communications interface (see paragraph 0035 and 0041-0046) coupled to said cryptographic processor (see figure 7);

Dellmo does not teach said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the

encapsulated communications module command packets to said communications module without performing cryptographic processing thereon.

Forslow teaches said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon (see Forslow figure 2 and column 9 lines 10-28). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have enclosed a command packet within an IP packet to have an efficient way to pass a command packet. Therefore one would be motivated to have enclosed a command packet within an IP packet.

With respect to 28, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036), and wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Mitsuoka figure 6A, 6B and column 14 lines 49-67).

With respect to claim 33, wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit (see Dellmo figure 4 paragraph Dellmo 0035 and 0041-0046).

With respect to claim 34, wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), and wherein said network communications interface comprises a network LAN interface (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 35, wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing (see Dellmo paragraph 0060).

With respect to claim 36 Dellmo teaches, a cryptographic module comprising: a user network interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices); a host network processor see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device) coupled to said user network interface (see figure 2); and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7);

Dellmo does not teach said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the

address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon.

Forslow teaches said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the address portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon (see Forslow figure 2 and column 9 lines 10-28). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have enclosed a command packet within an IP packet to have an efficient way to pass a command packet. Therefore one would be motivated to have enclosed a command packet within an IP packet.

With respect to claim 38, wherein the communications module command packets comprise Ethernet packets (see Dellmo paragraph 0035-0036).

With respect to 39, wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Mitsuoka figure 6A, 6B and column 14 lines 49-67).

With respect to claim 41, wherein said user network interface comprises an Ethernet Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA

Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices).

Claim 2, 22, 26, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Forslow (U.S. 6,973,057) in further view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols".

Dellmo Dichter and Mitsuoka teach everything with respect to claim 1, 21, 26 and 36 above but with respect to claim 2, 22, 26, and 37 they do not teach wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP). Stevens teaches wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP) (see Stevens page 359). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Simple Network Management Protocol to help manage the network (see page 359). Therefore one would have been motivated to have used Simple Network Management Protocol.

Claims 5, 6, 8, 11, 29, 30 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Forslow (U.S. 6,973,057) in further view of Cheng (U.S. 2003/0221034).

Dellmo and Forslow teach everything with respect to claim 1, and 26 above but with respect to claim 5, 6, 29 and 30 they do not teach wherein said cryptographic module further comprises: a first housing carrying said user network interface, said host

network processor, said cryptographic processor; and a first connector carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing carrying said network communications interface; and a second connector carried by said second housing and being removable mateable with said first connector of said cryptographic module. Cheng teaches wherein said cryptographic module further comprises: a first housing (see Cheng figure 4 element 51A) carrying said user network interface, said host network processor, said cryptographic processor; and a first connector (see Cheng figure 4 element 53A) carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing (see Cheng figure 4 element 51B) carrying said network communications interface; and a second connector (see Cheng figure 4 element 53B) carried by said second housing and being removable mateable with said first connector of said cryptographic module (see Cheng figure 4). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have made the communications module removable coupled with the cryptographic module to allow the user to change the module based on changing requirements (see paragraph 0030). Therefore one would have been motivated to have made the communications module removable coupled with the cryptographic module.

With respect to claim 8, wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (see Cheng figure 4 and paragraph 0029-0030).

With respect to claim 11, wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing (see Dellmo paragraph 0060).

With respect to claim 32, wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (see Cheng figure 4 and paragraph 0029-0030).

Claims 7, 31 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Forslow (U.S. 6,973,057) in further view of Hashimoto (U.S. 4,907,275).

Dellmo and Forslow teach everything with respect to claim 1, 26 and 36 above but with respect to claim 7, 31 and 40 they do not teach wherein said cryptographic processor comprises: an unencrypted data buffer circuit coupled to said host network processor; a cryptography circuit coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit coupled to said cryptography circuit. Hashimoto teaches wherein said cryptographic processor comprises: an unencrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said host network processor (see Hashimoto figure 2B element 12); a cryptography circuit (see Hashimoto figure 2B element 15) coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said cryptography circuit. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have encrypted data buffer circuit and an

unencrypted data buffer circuit to help control the data flow into and out of the cryptography circuit. (see column 3 line 57 – column 4 line 2). Therefore one would have been motivated to have an encrypted data buffer circuit coupled between said user network interface and said cryptography circuit; and an unencrypted data buffer circuit coupled between said cryptography circuit and said network communications interface.

Claims 12, 13, and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Forslow et al (U.S. 6,973,057) in further view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols".

Dellmo teaches with respect to claim 12, a cryptographic device comprising: a cryptographic module (paragraph 0038 i.e. cryptography circuit 70) and a communications module (paragraph 0038 i.e. wireless transceiver 50) coupled thereto (see figure 7); said cryptographic module comprising a user Local Area Network (LAN) interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices), a host network processor (see paragraph 0035 it is inherent that the user station 25 has a processor since it generates "plain text" to sent to the secure wireless LAN device (applicants cryptographic device)) coupled to said user LAN interface (see figure 2), and a cryptographic processor (see paragraph 0047 i.e. cryptography processor 72) coupled to said host network processor (see figure 7); said communications module comprising a network LAN interface (see paragraph 0035 and 0041-0046) coupled to said cryptographic processor (see figure 7);

Dellmo does not teach said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet, said host network processor formatting the data portions based upon the simple network management protocol (SNMP); said cryptographic processor stripping the addressing portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon.

Forslow teaches said host network processor generating cryptographic processor command packets for said cryptographic processor each comprising an address portion for addressing the cryptographic processor and a data portion, and encapsulating the command packets for said communication module in the data portions of a communications module command packet; said cryptographic processor stripping the addressing portion from each cryptographic processor command packet and passing the encapsulated communications module command packets to said communications module without performing cryptographic processing thereon (see figure 2 and column 9 lines 10-28). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have enclosed a command packet within an IP packet to have an efficient way to pass a command packet. Therefore one would be motivated to have enclosed a command packet within an IP packet.

Stevens teaches wherein said host network processor formats the data portions based upon the simple network management protocol (SNMP) (see Stevens page 359). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used Simple Network Management Protocol to help manage the network (see page 359). Therefore one would have been motivated to have used Simple Network Management Protocol.

With respect to claim 13 wherein the cryptographic processor command packets comprise Internet protocol (IP) packets (see Stalings page 418 lines 8-13).

With respect to claim 18, wherein said network communications interface comprises at least one of a wireless LAN (WLAN) communication circuit, a wireline communication circuit, and a fiber optic communication circuit (see Dellmo figure 4 paragraph 0035 and 0041-0046).

With respect to claim 19, wherein said user LAN interface comprises an Ethernet interface (see figure 7 element 27 PCMCIA Connector and paragraph 0034 i.e. interface connector 27 may be a PCMCIA connector or other similar connector that can readily interface to a number of possible LAN devices).

With respect to claim 20, wherein said cryptographic module further comprises a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing (see paragraph 0060).

Claims 14, 15 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Forslow (U.S. 6,973,057) in view of

Stevens "TCP/IP Illustrated, Volume 1 The Protocols" in further view of Cheng (U.S. 2003/0221034).

Dellmo, Forslow and Stevens teach everything with respect to claim 12 above but with respect to claim 14 and 15 they do not teach wherein said cryptographic module further comprises: a first housing carrying said user network interface, said host network processor, said cryptographic processor; and a first connector carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing carrying said network communications interface; and a second connector carried by said second housing and being removable mateable with said first connector of said cryptographic module. Cheng teaches wherein said cryptographic module further comprises: a first housing (see Cheng figure 4 element 51A) carrying said user network interface, said host network processor, said cryptographic processor; and a first connector (see Cheng figure 4 element 53A) carried by said first housing and coupled to said cryptographic processor; said communications module further comprises: a second housing (see Cheng figure 4 element 51B) carrying said network communications interface; and a second connector (see Cheng figure 4 element 53B) carried by said second housing and being removable mateable with said first connector of said cryptographic module (see Cheng figure 4). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have made the communications module removable coupled with the cryptographic module to allow the user to change the module based on changing requirements (see paragraph 0030). Therefore one would have been motivated to have made the communications module removable coupled with the cryptographic module.

With respect to claim 17, wherein said communications module comprises a predetermined one from among a plurality of interchangeable communications modules each for communicating over a different communications media (see Cheng figure 4 and paragraph 0029-0030).

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dellmo (U.S. Patent 2002/0095594) in view of Dichter (U.S. 6,401,115) in view of Mitsuoka et al (U.S. 7,127,543) in view of Stevens "TCP/IP Illustrated, Volume 1 The Protocols" in further view of Hashimoto (U.S. 4,907,275).

Dellmo, Forslow and Stevens teach everything with respect to claim 12 above but with respect to claim 16 they do not teach wherein said cryptographic processor comprises: an unencrypted data buffer circuit coupled to said host network processor; a cryptography circuit coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit coupled to said cryptography circuit. Hashimoto teaches wherein said cryptographic processor comprises: an unencrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said host network processor (see Hashimoto figure 2B element 12); a cryptography circuit (see Hashimoto figure 2B element 15) coupled to said unencrypted data buffer circuit; and an encrypted data buffer circuit (see Hashimoto figure 2B element 14) coupled to said cryptography circuit. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have encrypted data buffer circuit and an unencrypted data buffer circuit to help control the data flow into and out of the cryptography circuit. (see column 3 line 57 – column 4 line 2). Therefore one would have been motivated to have an encrypted data buffer circuit coupled between said user network interface and said

cryptography circuit; and an unencrypted data buffer circuit coupled between said cryptography circuit and said network communications interface.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432